

Application Serial No. 09/747,365

Claims 1-2 (Cancelled.)

3. (New) A method for a clearinghouse or routing policy server to securely enroll a client device for an Internet telephony or multi-media communication system, comprising the steps:

receiving a first message via HTTP from a client device that comprises a request to obtain an identity of one of a clearinghouse and routing policy server, the request further comprising a computer programming variable operation that is set equal to alphanumeric text comprising 'getcacert' that initiates a search for a certificate authority certificate;

responding to the request by transmitting a second message comprising the certificate authority certificate of one of a clearinghouse and routing policy server in a Base64 format and encoded in ASCII with content type set to text/html;

receiving a third message comprising a certificate request from the client device;

responding to the client device request by signing the certificate; and

transmitting a fourth message comprising the certificate signed by a certificate authority of one of the clearinghouse and the routing policy server.

4. (New) The method of Claim 3, wherein the second message comprises a programming variable status that is set equal to alphanumeric text comprising '0&certificate'.

5. (New) The method of Claim 3, wherein the third message further comprises a computer programming variable operation that is set equal to at least one of a nonce value, a user's name, a user's password, a device identifier, a customer identifier, and a certificate request to be signed.

6. (New) The method of Claim 3, wherein the fourth message further comprises a computer programming variable entitled status that is set equal to alphanumeric text comprising '0&certificate'.

Application Serial No. 09/747,365

7. (New) A method for a clearinghouse or routing policy server to securely enroll a client device for an Internet telephony or multi-media communication system, comprising the steps:

receiving a first message from a client device that comprises a request to obtain an identity of one of a clearinghouse and routing policy server;

responding to the request by transmitting a second message comprising a certificate authority certificate of one of a clearinghouse and routing policy server to the client device;

receiving a third message comprising a certificate request from the client device, the certificate request comprising a nonce value, a user's name, a user's password, a device identifier, a customer identifier, and a certificate request to be signed;

responding to the client device request by signing the certificate; and

transmitting a fourth message comprising the certificate signed by the certificate authority of one of the clearinghouse and routing policy server.

8. (New) The method of Claim 7, wherein the first message further comprises a computer programming variable entitled operation that is set equal to alphanumeric text comprising 'getcacert' that initiates a search for a certificate authority certificate.

9. (New) The method of Claim 7, wherein the first message further comprises a POST message received via HTTP.

10. (New) The method of Claim 7, wherein the second message further comprises certificate authority certificate in a Base64 format and encoded in ASCII with content type set to text/html.

11. (New) The method of Claim 7, wherein the second message further comprises a programming variable status that is set equal to alphanumeric text comprising '0&certificate'.

12. (New) The method of Claim 7, wherein the fourth message further comprises a computer programming variable entitled status that is set equal to alphanumeric text comprising '0&certificate'.

Application Serial No. 09/747,365

13. (New) A method for a clearinghouse or routing policy server to securely enroll a client device for an Internet telephony or multi-media communication system, comprising the steps:

receiving a first message from a client device that comprises a request to obtain an identity one of a clearinghouse and routing policy server;

responding to the request by transmitting a second message comprising a certificate authority certificate of one of a clearinghouse and a routing policy server to the client device, wherein the second message comprises a programming variable status that is set equal to alphanumeric text comprising 'O&certificate' that indicates certificate authority information follows the alphanumeric text;

receiving a third message comprising a certificate request from the client device comprising a certificate request to be signed;

responding to the client device request by signing the certificate; and

transmitting a fourth message comprising the certificate signed by the certificate authority of one of the clearinghouse and routing policy server.

14. (New) The method of Claim 13, wherein the first message further comprises a computer programming variable operation that is set equal to alphanumeric text comprising getcacert that initiates a search for a certificate authority certificate.

15. (New) The method of Claim 13, wherein the first message further comprises a POST message received via HTTP.

16. (New) The method of Claim 13, wherein the second message further comprises the certificate authority certificate in a Base64 format and encoded in ASCII with content type set to text/html.

17. (New) The method of Claim 13, wherein the third message further comprises a computer programming variable operation that is set equal to at least one of a nonce value, a user's name, a user's password, a device identifier, a customer identifier, and a certificate request to be signed.

Application Serial No. 09/747,365

18. (New) The method of Claim 13, wherein the fourth message further comprises a computer programming variable status that is set equal to alphanumeric text comprising '0&certificate'.

[The Remainder of this page has been intentionally left blank.]